etc.), about an individual that is maintained by a DoD Component, including, but not limited to, his or her education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(s) *Risk assessment*. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.

(t) *Routine use*. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

(u) *Source agency*. Any agency which discloses records contained in a system of records to be used in a computer matching program, or any state or local government, or agency thereof, which discloses records to be used in a computer matching program.

(v) *Statistical record*. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(w) *System of records*. A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

§ 310.5 Policy.

It is DoD policy that:

(a) The privacy of an individual is a personal and fundamental right that shall be respected and protected.

(1) The Department's need to collect, maintain, use, or disseminate personal information about individuals for purposes of discharging its statutory responsibilities shall be balanced against the right of the individual to be protected against unwarranted invasions of their privacy.

(2) The legal rights of individuals, as guaranteed by Federal law, regulation, and policy, shall be protected when collecting, maintaining, using, or disseminating personal information about individuals.

(3) DoD personnel, to include contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual.

(4) Departmental legislative, regulatory, or other policy proposals shall be evaluated to ensure that privacy implications, including those relating to the collection, maintenance, use, or dissemination of personal information, are assessed, to include, when required and consistent with the Privacy Provision of the E-Government Act of 2002 (44 U.S.C. 3501, Note), the preparation of a Privacy Impact Assessment.

(b) Personal information shall be collected, maintained, used, or disclosed to ensure that:

(1) It shall be relevant and necessary to accomplish a lawful DoD purpose required to be accomplished by statute or Executive order.

(2) It shall be collected to the greatest extent practicable directly from the individual.

(3) The individual shall be informed as to why the information is being collected, the authority for collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

(4) It shall be relevant, timely, complete, and accurate for its intended use; and

(5) Appropriate administrative, technical, and physical safeguards shall be established, based on the media (e.g., paper, electronic, etc.) involved, to ensure the security of the records and to prevent compromise or misuse during storage, transfer, or use, including working at authorized alternative worksites.

(c) No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as follows:

(1) When specifically authorized by statute;

(2) When expressly authorized by the individual on whom the record is maintained; or

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity.

(d) Notices shall be published in the FEDERAL REGISTER and reports shall be submitted to Congress and the Office of Management and Budget, in accordance with, and as required by, 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, as to the existence and character of any system of records being established or revised by the DoD Components. Information shall not be collected, maintained, used, or disseminated until the required publication and review requirements, as set forth in 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, are satisfied.

(e) Individuals shall be permitted, to the extent authorized by 5 U.S.C. 552a and DoD 5400.11–R, to:

(1) Determine what records pertaining to them are contained in a system of records.

(2) Gain access to such records and obtain a copy of those records or a part thereof.

(3) Correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete.

(4) Appeal a denial of access or a request for amendment.

(f) Disclosure of records pertaining to an individual from a system of records shall be prohibited except with the consent of the individual or as otherwise authorized by 5 U.S.C. 552a, DoD 5400.11–R, and DoD 5400.7–R. When disclosures are made, the individual shall be permitted, to the extent authorized by references 5 U.S.C. 552a and/or DoD 5400.11–R, to seek an accounting of such disclosures from the DoD Component making the release.

(g) Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency shall be prohibited to the extent authorized by Public Law 86–36 (1959) and 10 U.S.C. 424. Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units shall be prohibited to the extent authorized by 10 U.S.C. 130b. Disclosure of medical records is prohibited except as authorized by DoD 6025.18–R.[6]

(h) Computer matching programs between the DoD Components and the Federal, State, or local governmental agencies shall be conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(i) DoD personnel and system managers shall conduct themselves consistent with established rules of conduct 310.8 so that personal information to be stored in a system of records only shall be collected, maintained, used, and disseminated as is authorized by this part, 5 U.S.C. 552a and DoD 5400.11–R.

(j) DoD personnel, including but not limited to family members, retirees, contractor employees, and volunteers, shall be notified, in a timely manner, consistent with the requirements of DoD 5400.11–R, if their personal information, whether or not included in a system of records, is lost, stolen, or compromised.

(k) DoD Field Activities shall receive Privacy Program support from the Director, Washington Headquarters Services.

§ 310.6 Responsibilities.

(a) The Director of Administration and Management, Office of the Secretary of Defense, shall:

(1) Serve as the Senior Privacy Official for the Department of Defense.

(2) Provide policy guidance for, and coordinate and oversee administration of, the DoD Privacy Program to ensure compliance with policies and procedures in 5 U.S.C. 552a and OMB Circular A–130.

(3) Publish DoD 5400.11–R and other guidance, including Defense Privacy Board Advisory Opinions, to ensure timely and uniform implementation of the DoD Privacy Program.

(4) Serve as the Chair to the Defense Privacy Board and the Defense Data Integrity Board (see § 310.9).

(5) Supervise and oversee the activities of the Defense Privacy Office (see § 310.9).

[6] See footnote 1 to § 310.1.